SEGURIDAD INFORMÁTICA
(propuesta de investigación)

OBJETIVOS ESPECÍFICOS

- Conocer si se toman medidas de prevención en las empresas que manejan una alta cantidad de información
- Conocer que tan óptima es la seguridad de las empresa

OBJETIVO GENERAL

- Conocer si existe confiabilidad en los sistemas informáticos

JUSTIFICACION

El motivo por el cual seleccionamos ese tema es porque la informática siempre nos ha llamado la atención y porque los delitos informáticos están estrechamente relacionados con la informática de este modo debemos tener nociones de cómo combatirlos para compartir o guardar de forma segura nuestra información

ALCANCES Y LIMITES

Esta investigación está centrada en las empresas del sector financiero en el Municipio de El Carmen de Bolívar, de este modo se contará con un diseñado plan de trabajo para poder cubrir todo este sector

INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN

TIPO DE INVESTIGACIÓN

La investigación tiene un enfoque cuantitativo ya que se emplearía una encuesta como medio de recolección de datos, la cual nos arrojará unos resultados en forma de porcentajes, con el propósito de conocer en realidad si se implementan los mecanismos de seguridad en cualquier empresa

INTRODUCCIÓN

La presente propuesta tiene su origen en un problema concreto que es la forma en cómo es manejada la información dentro de una empresa y sus niveles de seguridad en las redes o en sistemas de información, el cual se ha enfrentado diariamente por el sector financiero, productivo, gobierno, instituciones, empresas y usuarios particulares; este es las vulnerabilidades de los sistemas de seguridad que permiten salvaguardar su información, o sea tener estrategias adecuadas para la seguridad cibernética; para lo que se ha realizado en esta propuesta las formas de ataques informáticos y cómo prevenirlos.

MARCO TEÓRICO

La propuesta tiene su origen en un problema concreto, radica en cómo es manejada la información dentro de una empresa y sus niveles de seguridad en las redes o en sistemas de información, el cual se ha enfrentado diariamente por el sector financiero, productivo, gobierno, instituciones, empresas y usuarios particulares

MARCO TEÓRICO

MARCO TEÓRICO

MARCO TEÓRICO

RESULTADOS ESPERADOS

RESULTADOS ESPERADOS

SEGURIDAD INFORMATIVA

La Seguridad Informática es una temática importante en nuestro campo como Ingenieros de Sistemas por ello nuestra investigación se centra en su estudio. A lo largo de la investigación observaremos como en nuestro trabajo y vida cotidiana se maneja un flujo de información continuo, muchos de estos datos son confidenciales, por ende necesitan ser manejados con la mayor discreción por ello se implementan medidas de seguridad como password y anti virus..

José Vargas Barreto
ING. Sistema
U. de Cartagena
El Carmen de Bolivar

SEGURIDAD INFORMÁTICA
(propuesta de investigación)

OBJETIVOS ESPECÍFICOS

- Conocer si se toman medidas de prevención en las empresas que manejan una alta cantidad de información
- Conocer que tan óptima es la seguridad de las empresa

OBJETIVO GENERAL

- Conocer si existe confiabilidad en los sistemas informáticos

INTRODUCCIÓN

La presente propuesta tiene su origen en un problema concreto que es la forma en cómo es manejada la información dentro de una empresa y sus niveles de seguridad en las redes o en sistemas de información, el cual se ha enfrentado diariamente por el sector financiero, productivo, gobierno, instituciones, empresas y usuarios particulares; este es las vulnerabilidades de los sistemas de seguridad que permiten salvaguardar su información, o sea tener estrategias adecuadas para la seguridad cibernética; para lo que se ha realizado en esta propuesta las formas de ataques informáticos y cómo prevenirlos.

SEGURIDAD INFORMATIVA

La Seguridad Informática es una temática importante en nuestro campo como Ingenieros de Sistemas por ello nuestra investigación se centra en su estudio. A lo largo de la investigación observamos como en nuestro trabajo y vida cotidiana se maneja un flujo de información continua, muchos de estos datos son confidenciales, por ende necesitan ser manejados con la mayor discreción por ello se implementan medidas de seguridad como password y anti virus..

JUSTIFICACION

El motivo por el cual seleccionamos este tema es porque la informática siempre nos ha llamado la atención y porque los delitos informáticos están estrechamente relacionados con la informática de este modo debemos tener nociones de cómo combatirlos para compartir o guardar de forma segura nuestra información

ALCANCES Y LIMITES

Esta investigación está centrada en las empresas del sector financiero en el Municipio de El Carmen de Bolívar, de este modo se contará con un diseñado plan de trabajo para poder cubrir todo este sector

MARCO TEÓRICO

La propuesta tiene su origen en un problema concreto, radica en cómo es manejada la información dentro de una empresa y sus niveles de seguridad en las redes o en sistemas de información, el cual se ha enfrentado diariamente por el sector financiero, productivo, gobierno, instituciones, empresas y usuarios particulares

MARCO TEÓRICO

MARCO TEÓRICO

MARCO TEÓRICO

TIPO DE INVESTIGACIÓN

La investigación tiene un enfoque cuantitativo ya que se emplearía una encuesta como medio de recolección de datos, la cual nos arrojará unos resultados en forma de porcentajes, con el propósito de conocer en realidad si se implementan los mecanismos de seguridad en cualquier empresa

INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN

INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN

RESULTADOS ESPERADOS

RESULTADOS ESPERADOS

José Vargas Barreto
ING. Sistema
U. de Cartagena
El Carmen de Bolivar

Prezi

SEGURIDAD INFORMATIVA

La Seguridad Informática es una temática importante en nuestro campo como Ingenieros de Sistemas por ello nuestra Investigación se centra en su estudio. A lo largo de la investigación observaremos como en nuestro trabajo y vida cotidiana se maneja un flujo de información continuo, muchos de estos datos son confidenciales, por ende necesitan ser manejados con la mayor discreción por ello se implementan medidas de seguridad como password y anti virus,,

INTRODUCCIÓN

La presente propuesta tiene su origen en un problema concreto que es la forma en cómo es manejada la información dentro de una empresa y sus niveles de seguridad en las redes o en sistemas de información, el cual se ha enfrentado diariamente por el sector financiero, productivo, gobierno, instituciones, empresas y usuarios particulares; este es las vulnerabilidades de los sistemas de seguridad que permiten salvaguardar su información, o sea tener estrategias adecuadas para la seguridad cibernética; para lo que se ha realizado en esta propuesta las formas de ataques informáticos y cómo prevenirlos.

OBJETIVO GENERAL

- Conocer si existe confiabilidad en los sistemas informáticos

OBJETIVOS ESPECÍFICOS

- Conocer si se toman medidas de prevención en las empresas que manejan una alta cantidad de información
- Conocer que tan óptima es la seguridad de las empresa

JUSTIFICACION

El motivo por el cual seleccionamos ese tema es porque la informática siempre nos ha llamado la atención y porque los delitos informáticos están estrechamente relacionados con la informática de este modo debemos tener nociones de cómo combatirlos para compartir o guardar de forma segura nuestra información

ALCANCES Y LIMITES

Esta investigación está centrada en las empresas del sector financiero en el Municipio de El Carmen de Bolívar, de este modo se contará con un diseñado plan de trabajo para poder cubrir todo este sector

MARCO TEÓRICO

La propuesta tiene su origen en un problema concreto, radica en cómo es manejada la información dentro de una empresa y sus niveles de seguridad en las redes o en sistemas de información, el cual se ha enfrentado diariamente por el sector financiero, productivo, gobierno, instituciones, empresas y usuarios particulares

MARCO TEÓRICO

MARCO TEÓRICO

DELITOS INFORMÁTICOS:

Hoy en día las comunicaciones se hacen más accesibles cada vez más a todo el mundo, razón por la cual (entre otras muchos otros factores más) estamos a la merced de los delitos en la red. Los riesgos que conlleva el ser víctima de alguno de ellos pueden ser desde algo mínimo hasta algo muy considerado como la afectación a infraestructuras gubernamentales o privadas. Es necesario, para las personas que conocemos este mundo de la computación, preocuparnos por los sistemas de seguridad para los usuarios y buscar diferentes estrategias para la protección contra este tipo de acciones sancionadas por el derecho penal.

¿QUÉ ES UN DELITO INFORMÁTICO?[1]

Se considera un "Delito informático" o "Crimen Electrónico"[2] a aquella acción conducta ilícita susceptible a ser sancionada por la ley, por medio del uso correcto de internet, que tiene como objetivo esencial el destruir y dañar computadoras, medios electrónicos y redes de internet. Los delitos informáticos, al igual que la tecnología evoluciona y se hace más complejo al pasar de los días, razón por la cual el término anterior se puede ampliar a la inclusión de delitos como el fraude, el robo, el chantaje, violación a los derechos de autor, pornografía infantil, sabotaje, la falsificación y principalmente la manipulación de transferencias bancarias. Con el desarrollo de la programación y el internet, los delitos informáticos se han vuelto más frecuentes y sofisticados, y con ello la seguridad completa no existe, dado que cuando se llega a presentar alguna situación de esta naturaleza, el usuario configura un sistema de seguridad para la amenaza presentada, pero al poco tiempo deja de ser funcional ya que el móvil del

[1] (2008). Definición de delito informático - Delitos Informáticos. Retrieved March 18, 2015, from http://www.delitosinformaticos.info/delitos_informaticos/definicion.html.
[2] (2003). Delito Electrónico Compilación - Revista INTER-FORUM. Retrieved March 18, 2015, from http://www.revistainterforum.com/espanol/pdfes/Compilacion-crimen-eletronico.pdf.

MARCO TEÓRICO

ciberdelincuente cambia, y con ello la probabilidad de una fuga importante de información del usuario.

CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS[3]

Dentro de las acciones legales en contra de esta nueva versión de delincuencia, se pueden dividir estas categorías de crímenes en dos grupos:

1. Como fin u objetivo.- Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos, spam, ataque masivos a servidores de Internet y generación de virus.
2. Como instrumento o medio.- Crímenes realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, pornografía infantil, pedofilia, etc.

SUJETOS ACTIVOS Y PASIVOS

Así como en la vida real, se les otorga una clasificación a los criminales por la forma de ejecución de sus crímenes, como por ejemplo, psicópatas, asesinos en serie etc., en el ciberespacio también sucede lo mismo, por las características específicas tales como la habilidad para el manejo de los sistemas o la realización de tareas que le facilitan el acceso a información sensible. En algunos casos la motivación del delito no es económica, sino simplemente el deseo de hacer conocer a otras personas o simplemente ejercitar sus conocimientos.

ACTIVOS

Son aquellos que poseen ciertas características que no presentan el denominador común en los delincuentes, generalmente los activos se encuentran en un campo laboral específico, ya sea que estén involucrados en el manejo de información sensible, o bien poseen la habilidad de manejo de los sistemas informáticos. Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco",

[3] Gallego Yuste, A. (2012). Delitos informáticos: Malware, fraudes y estafas a través de ... Retrieved from http://e-archivo.uc3m.es/bitstream/handle/10016/16868/pfc_alberto_gallego_yuste.pdf?sequence=1.

MARCO TEÓRICO

término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland. Esta categoría requiere que:

1. El sujeto activo del delito sea una persona de cierto estatus socioeconómico
2. Su comisión no pueda explicarse por falta de medios económicos, carencia de recreación poca educación, poca inteligencia, ni por inestabilidad emocional

PASIVOS

A diferencia del activo, el pasivo que se le dará el nombre de "víctima del delito", es aquella sobre la cual recaen las acciones en general que realiza el activo. Mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi.

Pueden ser individuos que laboran en instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información[4], generalmente conectados a otros equipos o sistemas externos.

[4] (2012). SISTEMAS DE INFORMACIÓNN AUTOMATIZADOS EN LA ... Retrieved March 18, 2015, from http://www.archivonacional.go.cr/memorias/2001/01.pdf.

TIPO DE INVESTIGACIÓN

La investigación tiene un enfoque cuantitativo ya que se empleara una encuesta como medio de recolección de datos, la cual nos arrojara unos resultados en forma de porcentajes, con el propósito de conocer en realidad si se implementan los mecanismos de seguridad en cualquier empresa

INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN

Los instrumentos fueron creados en la herramienta formularios de GOOGLE DRIVE

INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN

ENCUESTA DE SEGURIDAD INFORMICA

Mediante esta encuesta mediremos el grado de seguridad que tiene usted y su empresa a la hora de un ataque informatico

*Obligatorio

1. **Como es su nombre** *
   (Apellidos y Nombres)

   .....

2. **Alguna vez ha escuchado hablar de Seguridad Informatica**
   Marca solo un óvalo.

   - ◯ SI
   - ◯ NO

3. **Que cual de estos Antivirus utiliza su equipo**
   seleccione solo uno
   Marca solo un óvalo.

   - ◯ AVAST
   - ◯ ESET
   - ◯ Avira
   - ◯ AVG
   - ◯ Kapersky
   - ◯ McAfee

4. **Que tipo de seguridad personal tiene usted**
   puede elegir mas de una
   Selecciona todos los que correspondan.

   - ☐ No abre correos estraño
   - ☐ Ejecuta regularmente su antivirus
   - ☐ analiza la información enviada por correos
   - ☐ Hace caso omiso a publicidad estraña

5. **Comparte información confidencial con compañeros de trabajo**
   Marca solo un óvalo.

   - ◯ SI
   - ◯ NO

INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN

6. **Con que frecuencia comparte información con sus compañeros**
Marca solo un óvalo.

- ◯ Todos los dias
- ◯ Una ves a la semana
- ◯ Mas de una ves a la semana
- ◯ Mas de tres veces al mes

7. **Si le colocaran a elegir la fecha en la cual desearía que su equipo se revisara con mayor frecuencia.¿cual seria la mejor?**

Ejemplo: 15 de diciembre

8. **Califique en su opinión personal.**
siendo 1 el mas bajo y 5 el mas altoo
Marca solo un óvalo.

	1	2	3	4	5
Siente usted que su información esta proegida	◯	◯	◯	◯	◯

9. **Toma usted precauciónes a la hora de manipular algunas páginas web**
Marca solo un óvalo.

- ◯ Siempre
- ◯ Algunas veces
- ◯ Nunca

10. **Cual es la hora en la cual usted accede con frecuencia a su correo**

Ejemplo: 8:30 a.m.

11. **Con que frecuencia realiza las siguientes actividades**
Marca solo un óvalo por fila.

	Siempre	Algunas veces	Nunca
Utilización de antivirus en correos electronicos	◯	◯	◯
Desinfecciones de memorias USB	◯	◯	◯
Ejecución del antivirus de su equipo	◯	◯	◯
Apertura de correos estraños	◯	◯	◯
visualización de publicidad	◯	◯	◯

INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN

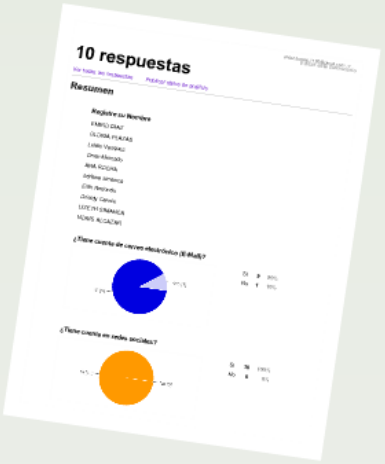
12. **Como mejoraría la seguridad suya y de su empresa**
sea breve

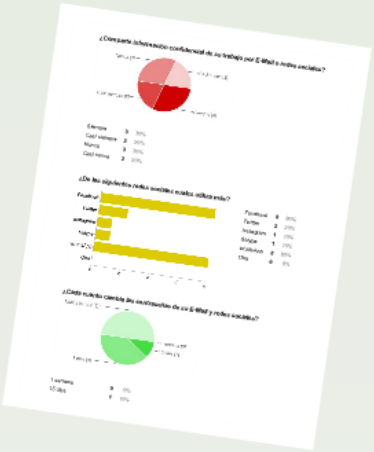
Con la tecnología de
Google Forms

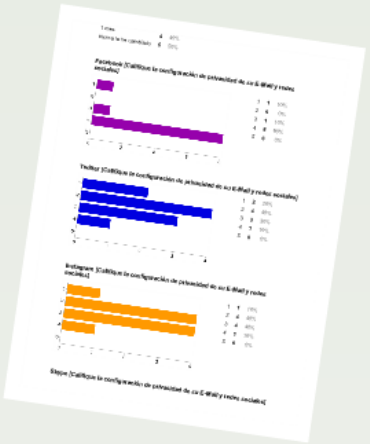
RESULTADOS ESPERADOS

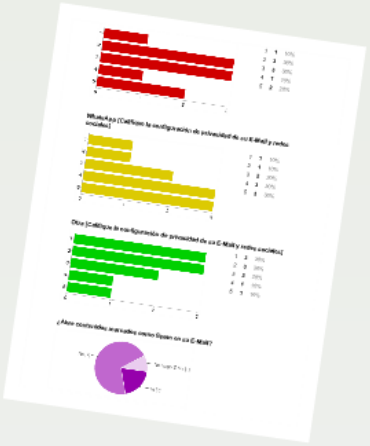
El principal objetivo que se espera de la encuesta que deseamos efectuar a los empleados, es reconocer si se da un buen uso de manejo de información o si por el contrario, los empleados no toman las precauciones necesarias para intercambiar datos

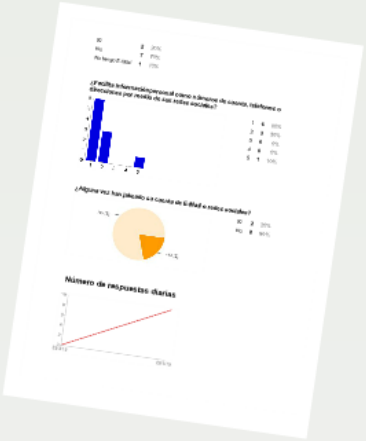
RESULTADOS ESPERADOS











José Vargas Barreto

ING. Sistema

U. de Cartagena

El Carmen de Bolivar

SEGURIDAD INFORMÁTICA

(propuesta de investigación)

OBJETIVOS ESPECÍFICOS

- Conocer si se toman medidas de prevención en las empresas que manejan una alta cantidad de información
- Conocer que tan óptima es la seguridad de las empresa

OBJETIVO GENERAL

- Conocer si existe confiabilidad en los sistemas informáticos

INTRODUCCIÓN

La presente propuesta tiene su origen en un problema concreto que es la forma en cómo es manejada la información dentro de una empresa y sus niveles de seguridad en las redes o en sistemas de información, el cual se ha enfrentado diariamente por el sector financiero, productivo, gobierno, instituciones, empresas y usuarios particulares; este es las vulnerabilidades de los sistemas de seguridad que permiten salvaguardar su información, o sea tener estrategias adecuadas para la seguridad cibernética; para lo que se ha realizado en esta propuesta las formas de ataques informáticos y cómo prevenirlos.

SEGURIDAD INFORMATIVA

La Seguridad Informática es una temática importante en nuestro campo como Ingenieros de Sistemas por ello nuestra investigación se centra en su estudio. A lo largo de la investigación observaremos como en nuestro trabajo y vida cotidiana se maneja un flujo de información continuo, muchos de estos datos son confidenciales, por ende necesitan ser manejados con la mayor discreción por ello se implementan medidas de seguridad como password y anti virus.

JUSTIFICACION

El motivo por el cual seleccionamos ese tema es porque la informática siempre nos ha llamado la atención y porque los delitos informáticos están estrechamente relacionados con la informática de este modo debemos tener nociones de cómo combatirlos para compartir o guardar de forma segura nuestra información

ALCANCES Y LIMITES

Esta investigación está centrada en las empresas del sector financiero en el Municipio de El Carmen de Bolívar, de este modo se contará con un diseñado plan de trabajo para poder cubrir todo este sector

MARCO TEÓRICO

La propuesta tiene su origen en un problema concreto, radica en cómo es manejada la información dentro de una empresa y sus niveles de seguridad en las redes o en sistemas de información, el cual se ha enfrentado diariamente por el sector financiero, productivo, gobierno, instituciones, empresas y usuarios particulares

INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN

TIPO DE INVESTIGACIÓN

La investigación tiene un enfoque cuantitativo ya que se empleará una encuesta como medio de recolección de datos, la cual nos arrojará unos resultados en forma de porcentajes, con el propósito de conocer en realidad si se implementan los mecanismos de seguridad en cualquier empresa

MARCO TEÓRICO

MARCO TEÓRICO

MARCO TEÓRICO

RESULTADOS ESPERADOS

RESULTADOS ESPERADOS

José Vargas Barreto
ING. Sistema
U. de Cartagena
El Carmen de Bolivar